UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MALIBU MEDIA, LLC, Plaintiff, v. JOHN DOES 1-5, Defendants.	Civil Action No. 12-CV-2954-NRB

DECLARATION OF TOBIAS FIESER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO SERVE THIRD PARTY SUBPOENAS PRIOR TO A RULE 26(f) CONFERENCE

I, TOBIAS FIESER, HEREBY DECLARE:

1. My name is Tobias Fieser.

2. I am over the age of 18 and am otherwise competent to make this declaration.

3. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.

4. I am employed by IPP, Limited ("IPP"), a company organized and existing under the laws of Germany, in its litigation support department.

5. Among other things, IPP is in the business of providing forensic investigation services to copyright owners.

6. As part of my duties for IPP, I routinely identify the Internet Protocol ("IP") addresses that are being used by those people that are using the BitTorrent protocol to reproduce, distribute, display or perform copyrighted works.

7. An IP address is a unique numerical identifier that is automatically assigned to an

internet user by the user's Internet Service Provider ("ISP").

8. ISPs keep track of the IP addresses assigned to their subscribers.

9. Only the ISP to whom a particular IP address has been assigned for use by its subscriber can correlate the IP address to a real person, the subscriber of the internet service.

10. From time to time, a subscriber of internet services may be assigned different IP addresses from their ISP. Accordingly, to correlate a person with an IP address the ISP also needs to know when the IP address was being used.

11. Many ISPs only retain the information sufficient to correlate an IP address to a person at a given time for a very limited amount of time.

12. Plaintiff retained IPP to identify the IP addresses that are being used by those people that are using the BitTorrent protocol and the internet to reproduce, distribute, display or perform Plaintiffs' copyrighted work.

13. IPP tasked me with implementing, monitoring, analyzing, reviewing and attesting to the results of the investigation.

14. During the performance of my duties, I used forensic software named INTERNATIONAL IPTRACKER v1.2.1 and related technology enabling the scanning of peer-to-peer networks for the presence of infringing transactions. A summary of how the software works is attached as Exhibit A.

15. INTERNATIONAL IPTRACKER v1.2.1 was correctly installed and initiated on a server located in the United States of America.

16. I personally extracted the resulting data emanating from the investigation.

17. After reviewing the evidence logs, I isolated the transactions and the IP addresses being used on the BitTorrent peer-to-peer network to reproduce, distribute, display or perform

Plaintiff's copyrighted work.

18. Through each of the transactions, the computers using the IP addresses identified on Exhibit B connected to the investigative server in order to transmit a full copy, or a portion thereof, of a digital media file identified by the hash value set forth on Exhibit B.

19. The IP addresses, hash values and hit dates contained on Exhibit B correctly reflect what is contained in the evidence logs.

20. The peers using the IP addresses set forth on Exhibit B were all part of a "swarm" of peers that were reproducing, distributing, displaying or performing the copyrighted work identified on Exhibit B.

21. Our software analyzed each BitTorrent "piece" distributed by each IP address listed on Exhibit B and verified that reassembling the pieces using a specialized BitTorrent Client results in a fully playable digital motion picture.

22. I was provided with a control copy of the copyrighted work identified on Exhibit B (the "Movie"). I viewed the Movie side-by-side with the digital media file identified by the hash value set forth on Exhibit B and determined that the digital media file contained a movie that was identical, striking similar or substantially similar.

23. Once provided with the IP address, plus the date and time of the detected and documented infringing activity, ISPs can use their subscriber logs to identify the name, address, email address, phone number and Media Access Control number of the subscriber.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 26th day of March, 2012.

TOBIAS FIESER

By: _____